

**MEDICAL RECORDS SECURITY**

**General Information**

Medical record security is closely linked to the general principles noted in Privacy & Access to Information but is dealt with here as a distinct issue.

Medical records may be maintained as paper-based or computer records. Regardless of the system, individual staff and management must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. Staff need to protect medical records against unauthorised access where those records are being stored or transmitted. Fax, e-mail and telephone messages client information should be treated with security equal to that applying to medical records.

Breach of Data Protection Act & Confidentiality may result in disciplinary action leading to dismissal.

**Responsibilities**

* All Staff
  + Ensure access to medical records is available to authorised personnel only
  + Ensure the safe and secure storage of all medical records in the Health Centre
  + Ensure the health centre is secure after hours
  + Attend to filing of medical information promptly
  + Ensure the return of medical records to filing cabinets/compactus occurs promptly after client information is accessed
* Ephedra Managers/Directors
  + Ensure staff are familiar with the intent of the Information Act, and practice accordingly.

**General Security and Storage**

All paper records containing personal or confidential information must be stored securely in locked cupboards when not in use. This is particularly important archived records

Staff need to ensure that clients and other visitors to the health centre will not have access to the medical records, pathology results and other papers containing personal health information are not left where they may be accessed by unauthorised persons.

Where applicable, computer screens need to be positioned in such a way to prevent unauthorised viewing of a client’s personal health information. Staff need to ensure that computers left unattended cannot be accessed by unauthorised persons.

**Release of Medical Records & Personal Information**

Medical records are not to be removed from the health centre. No personal information shall be given over the telephone unless it has been established that the caller is an authorised recipient of such information and they can give proof of identity.

No personal information should be left on voicemail or any other telephone answering device.

Medical records requiring disposal must be shredded to ensure confidentiality of information.

**Need to Know Principle**

This is a key concept in safeguarding information privacy. This principle holds that personal information should be used only for the purpose for which it has been collected. Non-clinical staff are required to limit their access to personal health information to the minimum necessary for the performance of their duties.

*The importance of basic observations such as not discussing clients publicly in a manner that would allow identification of individuals or groups cannot be overemphasised.*

**SystmOne/Emis – Clinical Systems**

Only authorised staff should access to the clinical system for the purpose of providing health care to clients. Staff members should utilise an individually assigned User ID, password and Smartcard and this should only be used by authorised staff member. While using SystmOne or Emis, if staff temporarily leaves the computer, the smartcard should be removed and Lock your Computer Screen should be activated.

Last Updated 17 March 2018